Phishing Attack on VTOP

CSE3501: Information Security Analysis and Audit

J Component Project

Shrivats Poddar | Shivam Singhal

19BCE0750 | 19BCE2112

F1 Slot

B.Tech. Computer Science and Engineering

School of Computer Science and Engineering

Vellore Institute of Technology

Vellore

November, 2021

Table of Contents:

Abstract

Motivation

In India, we see advertisements saying do not share your OTP, CVV or Passwords to any unauthorised person. But the question here arises why will someone share his personal information with someone else. When a person is made to give their personal details on fraudulent sources this is known as phishing.

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

Phishing is the easiest kind of cyber security attack that one can perform with basic knowledge and resources. The viability of this attack is conditioned on the user providing the information themselves. Even the most knowledgeable people fall victim to this attack.

The most common way of phishing is via emails, where the received emails are too good to be true like winning a lottery. Secondly they may perceive a sense of urgency saying that it is a limited time deal. Then it usually has hyperlinks or attachments that infect the victim's information.

Aim and Objective

To clone the college ERP Portal (VTOP) and plan a phishing attack on the college users (Faculty and Students), study the results and note down people's reactions.

Expected Outcome

We will have a real time statistics of how people who are even in the field of computer science can fall for this attack. Doing this, we will have a better understanding of this kind of attack and can come up with measures to prevent it.

We will see which kind of attack/ combination of attacks works against various user profiles such as naive users, intermediate users and experienced users.

Introduction

Phishing is the easiest implementation for any kind of cyber attack performed by someone. Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

In this project we aim to clone the college ERP Portal (VTOP) and plan a phishing attack on the college users (Faculty and Students), study the results and note down people's reactions. Based on the reactions come up with solutions and prevention mechanisms for the same.

Smishing is sending a message that requires someone to take action. This is the next evolution of vishing. Often the text includes a link that, when clicked, installs malware on the user's device. What we have done here in the project is called Smishing. It is a text based type of phishing.

A phishing attack can take various forms, and while it often takes place over email, there are many different methods scammers use to accomplish their schemes. This is especially true today as phishing continues to evolve in sophistication and prevalence. While the goal of any phishing scam is always stealing personal information, there are many different types of phishing you should be aware of.

1. Email Phishing

Arguably the most common type of phishing, this method often involves a "spray and pray" technique in which hackers impersonate a legitimate identity or organization and send mass emails to as many addresses as they can obtain.

These emails are often written with a sense of urgency, informing the recipient that a personal account has been compromised and they must respond immediately. Their objective is to elicit a certain action from the victim such as clicking a malicious link that leads to a fake login page. After entering their credentials, victims unfortunately deliver their personal information straight into the scammer's hands.

2. Spear Phishing

Rather than using the "spray and pray" method as described above, spear phishing involves sending malicious emails to specific individuals within an organization. Rather than sending out mass emails to thousands of recipients, this method targets certain employees at specifically chosen companies. These types of emails are often more personalized in order to make the victim believe they have a relationship with the sender.

3. Whaling

Whaling closely resembles spear phishing, but instead of going after any employee within a company, scammers specifically target senior executives (or "the big fish," hence the term whaling). This includes the CEO, CFO or any high-level executive with access to more sensitive data than lower-level employees. Often, these emails use a high-pressure situation to hook their victims, such as relaying a statement of the company being sued. This entices recipients to click the malicious link or attachment to learn more information.

4. Smishing

SMS phishing, or smishing, leverages text messages rather than email to carry out a phishing attack. They operate much in the same way as email-based phishing attacks: Attackers send texts from what seem to be legitimate sources (like trusted businesses) that contain malicious links. Links might be disguised as a coupon code (20% off your next order!) or an offer for a chance to win something like concert tickets.

5. Vishing

Vishing—otherwise known as voice phishing—is similar to smishing in that a phone is used as the vehicle for an attack, but instead of exploiting victims via text message, it's done with a phone call. A vishing call often relays an automated voice message from what is meant to seem like a legitimate institution, such as a bank or a government entity.

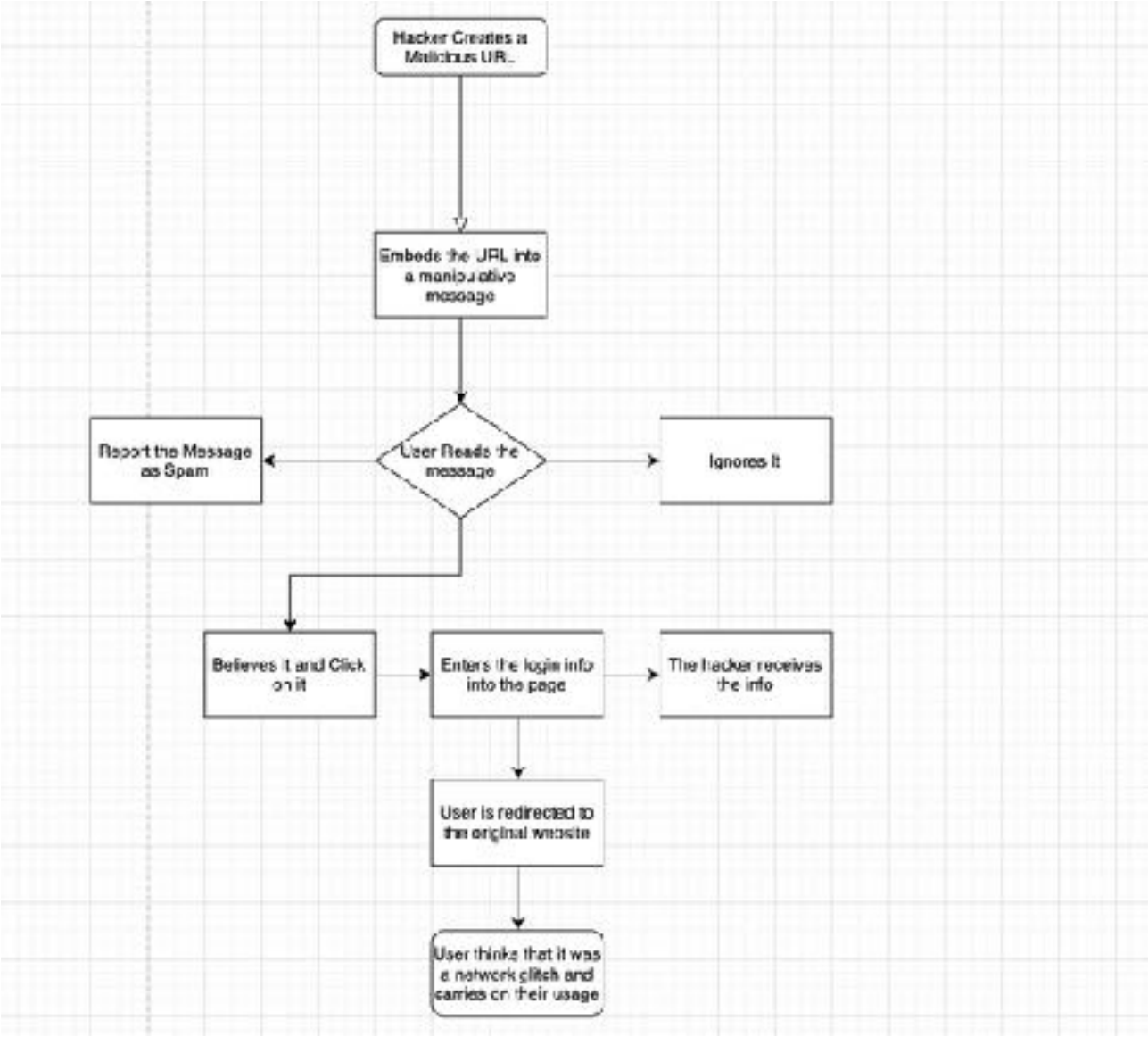
Attackers might claim you owe a large amount of money, your auto insurance is expired or your credit card has suspicious activity that needs to be remedied immediately. At this point, a victim is usually told they must provide personal information such as credit card credentials or their social security number in order to verify their identity before taking action on whatever claim is being made.

Literature Survey

- Abbasi, A., Dobolyi, D., Vance, A. and Zahedi, F.M., 2021. The phishing funnel model: A design artifact to predict user susceptibility to phishing websites. *Information Systems Research*, *32*(2), pp.410-436.
- Parno, B., Kuo, C. and Perrig, A., 2006, February. Phoolproof phishing prevention. In *International conference on financial cryptography and data security* (pp. 1-19). Springer, Berlin, Heidelberg.
- Gandotra, E. and Gupta, D., 2021. An Efficient Approach for Phishing Detection using Machine Learning. In *Multimedia Security* (pp. 239-253). Springer, Singapore.
- Jain, A.K. and Gupta, B.B., 2018. PHISH-SAFE: URL features-based phishing detection system using machine learning. In *Cyber Security* (pp. 467-474). Springer, Singapore.
- Jain, A.K. and Gupta, B.B., 2018. Towards detection of phishing websites on client-side using machine learning based approach. *Telecommunication Systems*, *68*(4), pp.687-700.
- Abbasi, A., Dobolyi, D., Vance, A. and Zahedi, F.M., 2021. The phishing funnel model: A design artifact to predict user susceptibility to phishing websites. *Information Systems Research*, *32*(2), pp.410-436.
- Parno, B., Kuo, C. and Perrig, A., 2006, February. Phoolproof phishing prevention. In *International conference on financial cryptography and data security* (pp. 1-19). Springer, Berlin, Heidelberg.
- Jain, A.K. and Gupta, B.B., 2018. PHISH-SAFE: URL features-based phishing detection system using machine learning. In *Cyber Security* (pp. 467-474). Springer, Singapore
- Jansson, K. and von Solms, R., 2013. Phishing for phishing awareness. *Behaviour & information technology*, *32*(6), pp.584-593.
- Dhamija, R., Tygar, J.D. and Hearst, M., 2006, April. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590).
- Fette, I., Sadeh, N. and Tomasic, A., 2007, May. Learning to detect phishing emails. In *Proceedings of the 16th international conference on World Wide Web* (pp. 649-656).
- Jansson, K. and von Solms, R., 2013. Phishing for phishing awareness. *Behaviour & information technology*, *32*(6), pp.584-593.
- Dhamija, Rachna, J. Doug Tygar, and Marti Hearst. "Why phishing works." In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pp. 581-590. 2006.

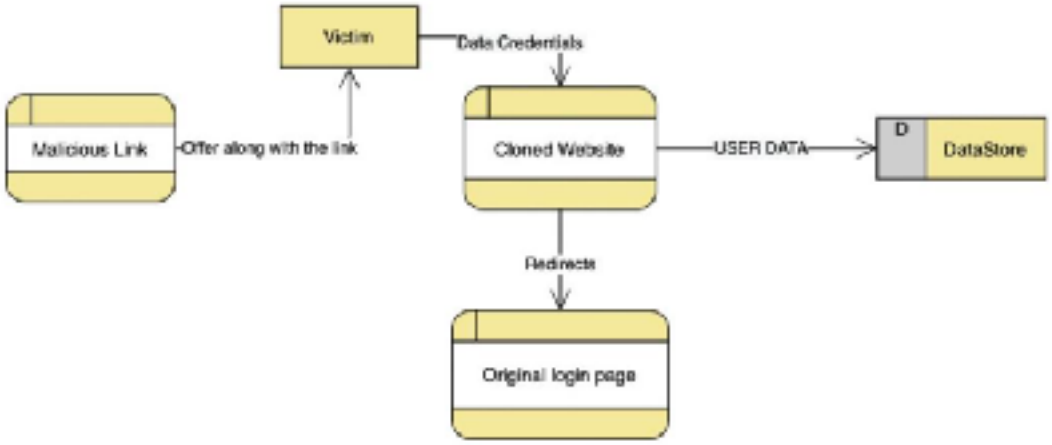
- Zhang, Y., Egelman, S., Cranor, L. and Hong, J., 2007. Phinding phish: Evaluating anti-phishing tools.
- Khonji, M., Iraqi, Y. and Jones, A., 2013. Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), pp.2091-2121.
- Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J. and Zhang, C., 2009. An empirical analysis of phishing blacklists.
- Akerlof, G.A. and Shiller, R.J., 2015. *Phishing for phools*. Princeton University Press.
- Abu-Nimeh, S., Nappa, D., Wang, X. and Nair, S., 2007, October. A comparison of machine learning techniques for phishing detection. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 60-69).
- Moghimi, M. and Varjani, A.Y., 2016. New rule-based phishing detection method. *Expert systems with applications*, *53*, pp.231-242.
- Medvet, E., Kirda, E. and Kruegel, C., 2008, September. Visual-similarity-based phishing detection. In *Proceedings of the 4th international conference on Security and privacy in communication netowrks* (pp. 1-6)

Overall Architecture



Flow chart of the Website

Data Flow Diagram



1. Malicious Link: This is a manual process, that the hacker performs to bait the victim in his attack. It consists of offers, click baits, lottery tickets etc. This is delivered to the victim.
2. Cloned Website: This is a replica of a site that looks like the real website of the source (VTop in this case). User can enter the user id and password and as he submits, the information is sent to the hacker.
3. Data Store: Store the stolen Data
4. Original Login Page: On clicking the submit button the user is redirected to the website's original page and is made to believe that everything is working smoothly. **In our case instead of this page issued a disclaimer alert saying, prevent phishing and do not click on malicious links. Requesting you to kindly change your password as its now stored with us now.

Methodology

Steps of a Phishing Attack

Step 1: The Information (Bait)

The first of the three steps of a phishing attack is preparing the bait. This involves finding out details about the target, which can be as simple as knowing that they use a particular service or work at a particular business. This is one of the reasons why data breaches where no 'sensitive' information is compromised can be so dangerous: if a service leaks a list of just email addresses of its users, criminals will be able to know that all the owners of those email addresses use that service and can target them with emails that pretend to be from that service.

Our Message Bait

In more sophisticated spear phishing attacks, cyber criminals can harvest details from your social media profiles in order to build a highly customised spear phishing message that is highly likely to convince you of its genuineness.

If you look closely the above URL its meant to look like the original URL - vtop.vit.ac.in. Illusion is the key to make the victim fall for phishing. So the bait should be as good as true for the attack to go successfully.

Step 2: The Promise (Hook)

Once the attacker has acquired the necessary information to use as bait, they then need to lay out the hook. In order to actually make the target perform an action, the attacker needs to promise something or scare them into action.

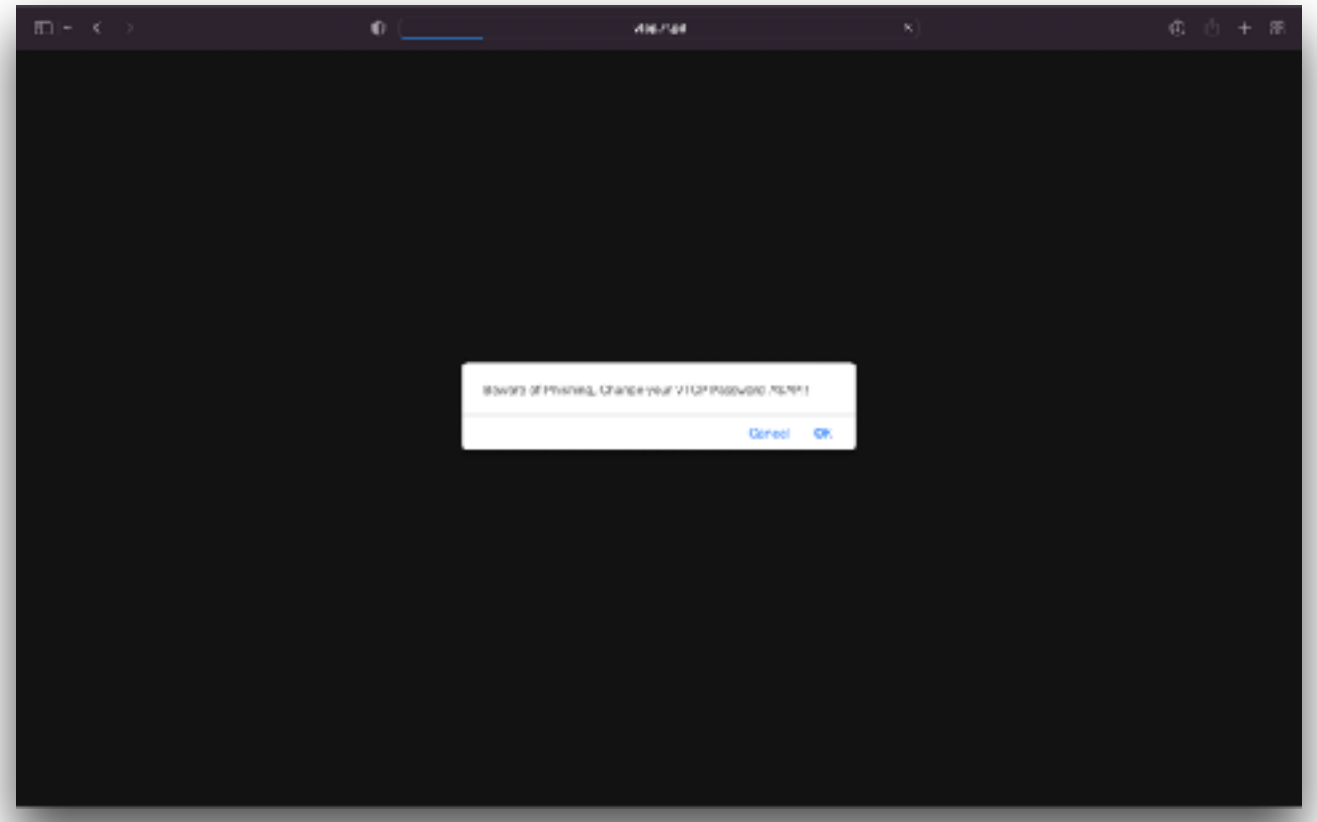
In the message above if you see the promise was to give access to the portal that was down for sever maintenance for 48 hrs. It is this kind of opportunity that an attacker look for to put out an attack.

In many other scams the hook involves making the target believe that one of their accounts have been compromised, creating a sense of urgency and making the target act quickly - perhaps without thinking. The attacker can then redirect the target to follow a link to a page where they can harvest the victim's details.

Step 3: The Attack (Catch)

The third phase of phishing is the actual attack. The cyber criminal sends out the email, and prepares for the prey to fall for the bait.

What the attacker's next action will be will depend on the nature of the scam. For example, if they used a landing page to gain the victim's email password, they can then log in to the victim's email account in order to harvest more information and start sending further phishing emails to the victim's contacts.



Disclaimer Added to inform the user that he/she was attacked

Results

+ Options

Username	Password
123	123
SADFSF	asdfsgf
19BCE0747	BQMF12345
19BCE1234	1234
19BCE2009	QWERTY1234
H	h
20BCB0086	ilovearsh2001
TP	afasfsafsaf
19BCE012	hithere
19BCB0086	password1
23456	qwerty
19BCE2000	sarthak
19BCE2024	Vansh23
19BCE0024	shivakumar12
19BCE2000	shivakumar12
19BCE2000	shivkumar12
19BCE2222	kimono234

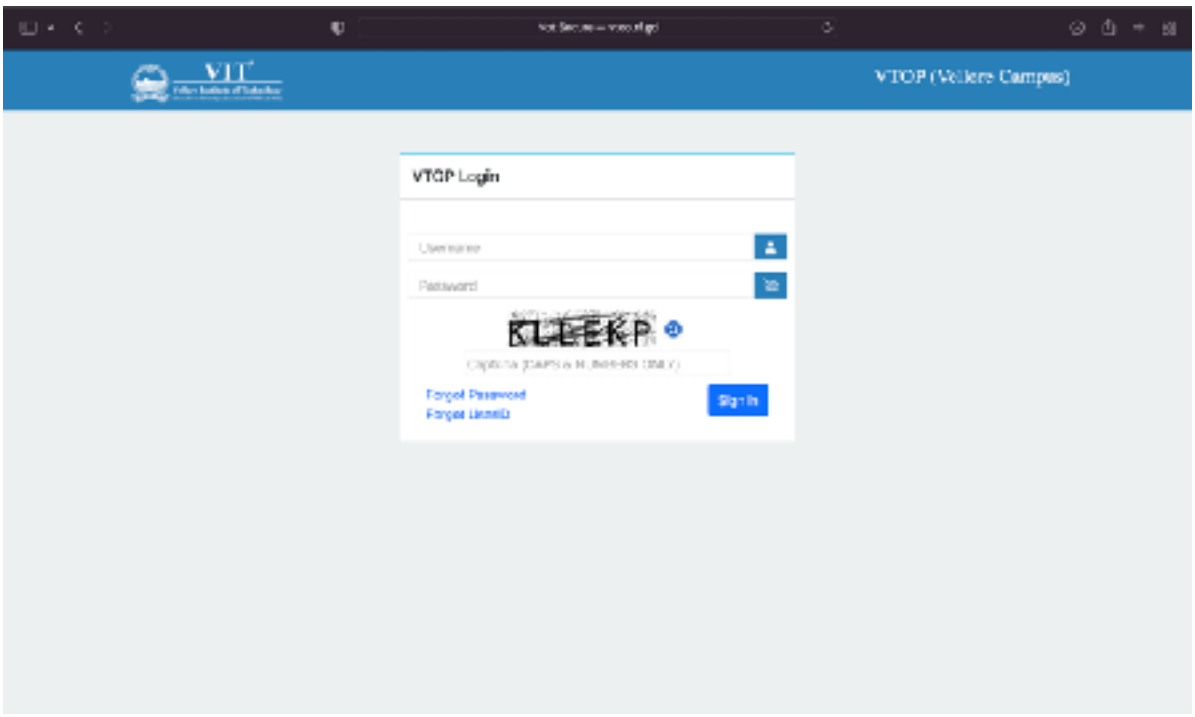
Screenshot of the Data Gathered on the Attacker Side

The attack was done on a closed group of engineering students probably in their second or third year of University pursuing a course in Computer Science and Engineering. This is the set of people who should be most careful of this kind of attack, but in crisis they let their guard down.

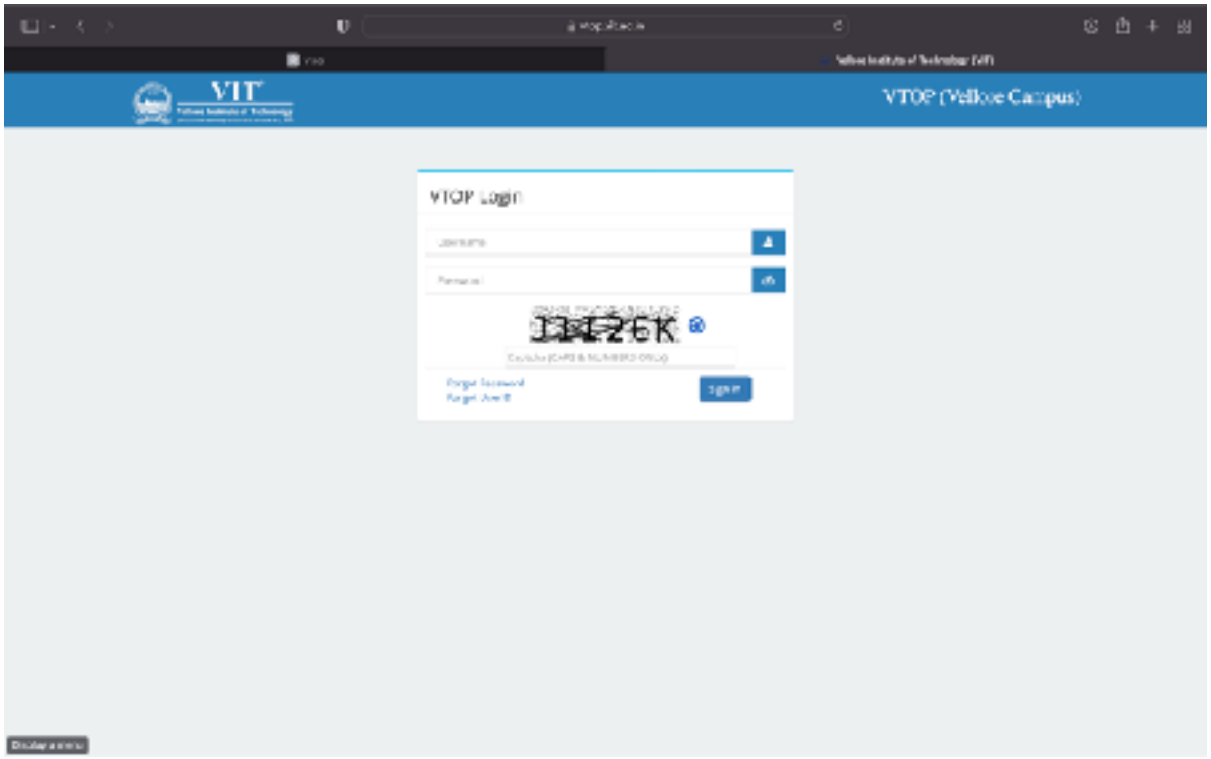
Analysis

In performing this attack we considered many details.

First we prepared a website clone that looked same as the official portal (Screenshots attached).



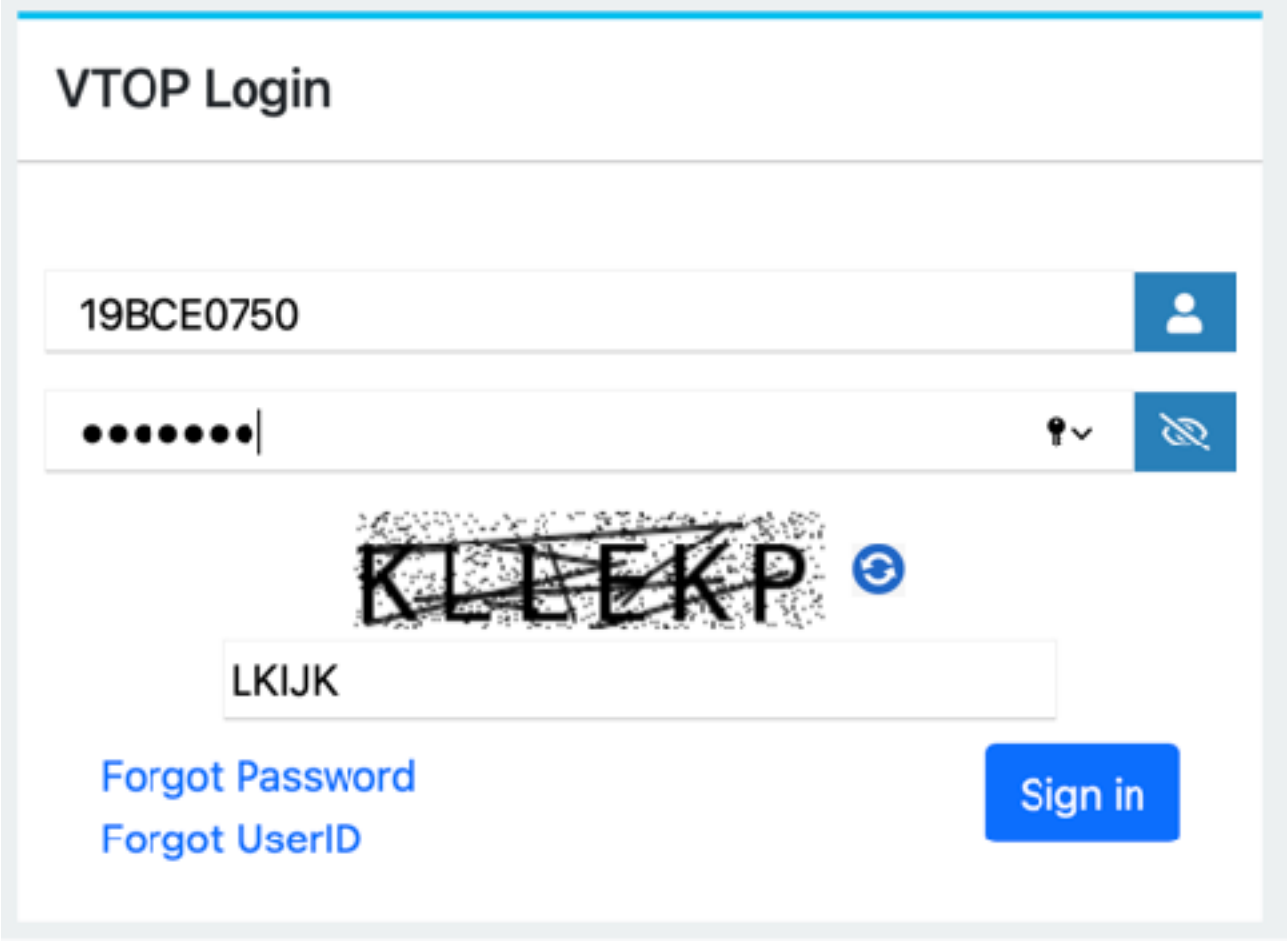
Website Clone



Real Website

- All the buttons are functional and provides same response as the original website did.

- As you can see there is a human verification captcha as well. This captcha has been designed to accept any response as true, as true.
- Like the original website the letters of the username and the capcha auto capitalises to reduce the risk of getting caught.
- The website the attacker shows is an illusion of what is true. And he has to master it for the victim to fall for the attack.
- As soon as the victim clicks the sign in button the username and password data is stored with the attacker.



A closer look at the form

Next after hosting the website the big thing is working with the URL and getting domain name. In our project we managed to get a close enough URL for people to believe in it.

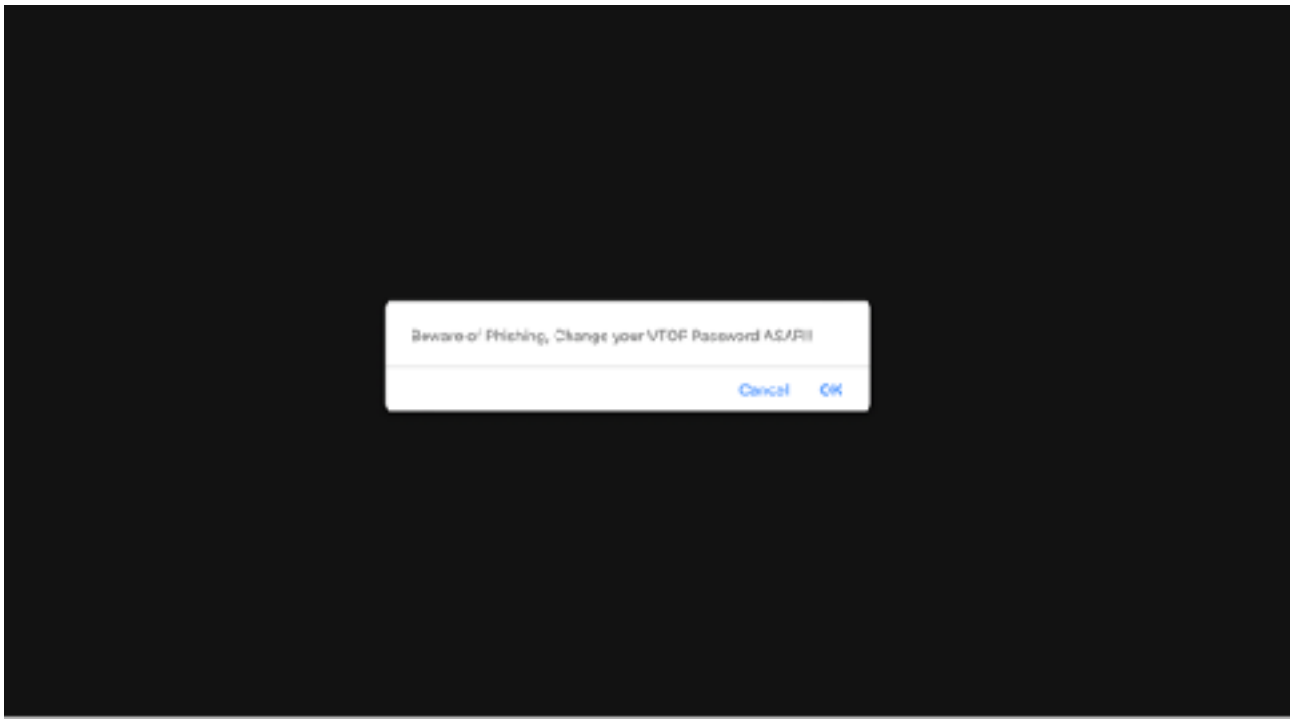
Original URL: vtop.vit.ac.in/

Clone URL: vtop.rf.gd/

- If you see the of making your URL (bait) to work is simplicity.
- The URL looks close enough to the original one for the victim to mistake it for the original URL.
- Also the formatting matches the formatting of the original URL.

Once the user clicked the sign in button he/she would be redirected to the VTOP's homepage believing that there has been a network glitch and carry on the activity.

But since this is an ethical project we added a little disclaimer saying that you have been attacked and kindly change your password asap.



So this disclaimer tells the concerned victim that he has been attacked and asks him to take immediate action on this.

Prevention of Phishing

Some ways to prevent phishing are:-

Know what a phishing scam looks like

New phishing attack methods are being developed all the time, but they share commonalities that can be identified if you know what to look for. There are many sites online that will keep you informed of the latest phishing attacks and their key identifiers. The earlier you find out about the latest attack methods and share them with your users through regular security awareness training, the more likely you are to avoid a potential attack.

Don’t click on that link

It’s generally not advisable to click on a link in an email or instant message, even if you know the sender. The bare minimum you should be doing is hovering over the link to see if the destination is the correct one. Some phishing attacks are fairly sophisticated, and the destination URL can look like a carbon copy of the genuine site, set up to record keystrokes or steal login/credit card information. If it’s possible for you to go straight to the site through your search engine, rather than click on the link, then you should do so.

Get free anti-phishing add-ons

Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there’s no reason not to have this installed on every device in your organization.

Don’t give your information to an unsecured site

If the URL of the website doesn’t start with “https”, or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Site’s without security certificates may not be intended for phishing scams, but it’s better to be safe than sorry.

Rotate passwords regularly

If you’ve got online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.

Don’t ignore those updates

Receiving numerous update messages can be frustrating, and it can be tempting to put them off or ignore them altogether. Don’t do this. Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack methods by patching holes in security. If

you don’t update your browser, you could be at risk of phishing attacks through known vulnerabilities that could have been easily avoided.

Install firewalls

Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

8. Don’t be tempted by those pop-ups

Pop-ups aren’t just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups. If one does manage to evade the ad-blocker though, don’t be tempted to click! Occasionally pop-ups will try and deceive you with where the “Close” button is, so always try and look for an “x” in one of the corners.

Don’t give out important information unless you must

As a general rule of thumb, unless you 100% trust the site you are on, you should not willingly give out your card information. Make sure, if you have to provide your information, that you verify the website is genuine, that the company is real and that the site itself is secure.

Have a Data Security Platform to spot signs of an attack

If you are unfortunate enough to be the victim of a successful phishing attack, then it’s important you are able to detect and react in a timely manner. Having a data security platform in place helps take some of the pressure off the IT/Security team by automatically alerting on anomalous user behavior and unwanted changes to files. If an attacker has access to your sensitive information, data security platforms can help to identify the affected account so that you can take actions to prevent further damage.

Conclusion

Phishing is the easiest kind of cyber security attack for any attacker and anyone with basic knowledge of web development can start this attack. There are softwares and programs that are constantly working on preventing phishing but as the prevention mechanisms upgrade so do the attacking methods. The best way to prevent phishing is by staying alert and be careful while opening malicious link.

References

1. Source Site: vtop.vit.ac.in/
2. Web Hosting: https://infinityfree.net/
3. https://www.pandasecurity.com/en/mediacenter/tips/types-of-phishing/
4. https://blog.usecure.io/three-steps-of-phishing
5. https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/
6. https://www.phishing.org/
7. https://dl.acm.org/doi/abs/10.1145/1124772.1124861
8. https://dl.acm.org/doi/abs/10.1145/1242572.1242660
9. https://ieeexplore.ieee.org/abstract/document/6497928
10. https://www.tandfonline.com/doi/abs/10.1080/0144929X.2011.632650
11. https://www.tomsguide.com/news/whatsapp-hijack-attack
12. https://www.indiatvnews.com/technology/news-caught-in-online-money-scam-cybercrime-expert-tells-you-what-to-do-next-679882
13. https://www.bgr.in/how-to/alert-new-paytm-cashback-scam-this-fake-paytm-site-fraudsters-trick-to-steal-your-money-check-details-963102/
14. https://www.rd.com/article/amazon-scams/

Appendix 1

Name	Registration No.	Work Done
Shrivats Poddar	19BCE0750	Found a URL, created a database to store the stolen data, hosted the the website
Shivam Singhal	19BCE2112	Cloned the Website's front end, keeping in mind all the buttons and elements

Appendix 2

Project files link:

https://github.com/shrivatspoddar/vtopPhishingClone